Oracle® Key Manager 3

Guía de descripción general y planificación

Versión 3.0.2

E52228-02

Abril de 2015



Oracle® Key Manager 3

Guía de descripción general y planificación

E52228-02

Tabla de contenidos

Lista de figuras

Lista de tablas

Prólogo

En esta guía, se proporciona una descripción general e información de planificación, y se identifican los requisitos para implementar Oracle Key Manager (OKM).

Accesibilidad a la documentación

Para obtener información sobre el compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso a My Oracle Support

Los clientes de Oracle que hayan contratado servicios de soporte electrónico pueden acceder a ellos mediante My Oracle Support. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o, si tiene alguna discapacidad auditiva, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`.

1

Planificación de la instalación

Utilice la siguiente lista de comprobación para planificar la instalación de OKM.

Revisión de la descripción general y las configuraciones de OKM

- Capítulo 2, *Descripción general de OKM* .
- Capítulo 3, *Configuraciones de OKM* .

Revisión de los requisitos del servidor

- Revise las especificaciones del dispositivo de gestión de claves (Sección 2.2.1, “Servidor del dispositivo de gestión de claves para OKM 3.0”).
- Revise las especificaciones de rack del dispositivo de gestión de claves (Sección 2.2.3, “Especificaciones de rack ”).
- Asegúrese de que el sitio cumpla con los requisitos de temperatura, humedad, enfriamiento y alimentación para el servidor.
    - Para conocer las especificaciones del servidor Netra SPARC T4-1, consulte:

      http://docs.oracle.com/cd/E23203_01/index.html
    - Verifique las ubicaciones y capacidades nominales de los disyuntores.
    - Para la opción de energía redundante, asegúrese de que haya un interruptor de energía APC adicional.

Revisión de los requisitos de red

- Capítulo 4, *Redes de OKM* .

Revisión de los requisitos de unidad de cinta

- Capítulo 5, *Requisitos de unidad de cinta*.

Planificación de roles de usuario

- Sección 2.8, “Roles de usuario”.

Preparación para la entrega

- Asegúrese de que haya personal autorizado disponible para organizar y aceptar la entrega. El dispositivo de gestión de claves (KMA) de OKM se considera un elemento seguro.
- Asegúrese de que exista un plan para desechar o reciclar el material de embalaje.

Pedido de componentes

- Capítulo 6, *Realización de pedidos* .

2

Descripción general de OKM

OKM proporciona seguridad de datos mediante el cifrado de los datos almacenados (cifrado basado en dispositivos). Crea, almacena y gestiona claves de cifrado. OKM admite sistemas abiertos y plataformas empresariales.

En las siguientes secciones, se describen los conceptos y los componentes de la solución OKM.

- Estándares de cifrado admitidos
- Dispositivo de gestión de claves (KMA)
- GUI de OKM
- CLI de OKM
- Cluster de OKM
- Agentes
- Unidades de datos, claves, políticas de claves y grupos de claves
- Roles de usuario
- Integración de IBM ICSF

2.1. Estándares de cifrado admitidos

OKM se basa en los siguientes estándares de la industria:

- FIPS PUB 140-2: requisitos de seguridad para módulos criptográficosFIPS PUB 46-3: estándar de cifrado de datosFIPS PUB 171: gestión de claves
- NIST 800-57 parte 1: recomendaciones para la gestión de claves
- IEEE 1619.1: estándar para el cifrado de cintas (completo)IEEE 1619.2: estándar para el cifrado de discos (en proceso)IEEE 1619.3: estándar para la gestión de claves (en curso)
- Criterios comunes (CC)
- ISO/IEC 1779: técnicas de seguridad
- Cifrado CCM–AES-256
- Cifrado simétrico
- Nonce
- Conjunto de cifrado (TLS 1.0, 2048-bit RSA, SHA1, HMAC)

2.2. Dispositivo de gestión de claves (KMA)

El dispositivo de gestión de claves es un servidor de seguridad reforzado que proporciona gestión de claves de ciclo de vida basada en políticas, autenticación, control de acceso y servicios de suministro de claves. El dispositivo de gestión de claves garantiza que todos los dispositivos de almacenamiento estén registrados y autenticados, y que toda creación, suministro y supresión de claves de cifrado se lleve a cabo de conformidad con las políticas establecidas.

2.2.1. Servidor del dispositivo de gestión de claves para OKM 3.0

OKM 3.0 es compatible con Solaris 11 en el servidor Netra SPARC T4-1. La versión de OKM de este servidor incluye:

- Procesador SPARC T4 de 4 núcleos y 2.85 GHz
- 32 GB de DRAM (4 DIMM de 8 GB)
- Unidad de disco SAS de 2,5 in con 600 GB a 10.000 rpm
- 4 puertos Gigabit Ethernet
- Fuentes de alimentación redundantes
- 5 ranuras de adaptador PCIe de segunda generación (con 8 vías cada una)
- Unidad de DVD (deshabilitada: no se usa con OKM)

Para conocer otras especificaciones del servidor, como los requisitos ambientales y de energía, consulte:

http://docs.oracle.com/cd/E23203_01/index.html

2.2.2. Servidores del dispositivo de gestión de claves para OKM 2.x

OKM 2.x es compatible con Solaris 10 en Sun Fire X2100 M2, X2200 M2 y X4170 M2.

Nota:

Los dispositivos de gestión de claves de Sun Fire no se pueden actualizar a OKM 3.0, pero se pueden comunicar con los dispositivos de gestión de claves de OKM 3.0 en el mismo cluster. Los dispositivos de gestión de claves de OKM 3.0 se pueden unir a un cluster de OKM 2.x existente mediante un dispositivo de gestión de claves que ejecute KMS 2.2 o posterior.

2.2.3. Especificaciones de rack

Los dispositivos de gestión de claves se pueden instalar en armarios o racks RETMA estándar de cuatro pilares y 19 in. No se admiten racks de dos pilares.

Nota:

La biblioteca SL8500 ofrece espacio para cuatro racks de 19 in. Para obtener más información, consulte la *Guía de aseguramiento de sistemas StorageTek SL8500*.

Las guías deslizantes son compatibles con racks con los siguientes estándares:

- Abertura horizontal y extremo vertical de la unidad que cumplen con los estándares ANSI/EIA 310-D-1992 o IEC 60927.
- Distancia entre los planos de montaje frontal y posterior entre 610 mm y 915 mm (24 in a 36 in).
- Profundidad de separación hasta la puerta delantera del armario de al menos 25,4 mm (1 in).
- Profundidad de separación hasta la puerta posterior del armario de al menos 800 mm (31,5 in) con un organizador de cables o 700 mm (27,5 in) sin un organizador de cables.
- Ancho de separación entre los soportes estructurales y los canales de cables, y entre los planos de montaje delantero y posterior, de al menos 456 mm (18 in).

2.2.4. Tarjeta SCA6000

La tarjeta Sun Cryptographic Accelerator (SCA6000) opcional se utiliza para las funciones administrativas y de procesamiento criptográfico requeridas para el cumplimiento con FIPS. Se trata de un módulo de seguridad de hardware FIPS 140-2 nivel 3.

2.3. GUI de OKM

Puede usar la GUI de OKM para configurar y gestionar OKM. Se ejecuta en una estación de trabajo proporcionada por el cliente y se comunica con los dispositivos de gestión de claves a través de una red IP. No se necesitan privilegios de administrador (Windows) o de usuario root (Solaris) para instalar y ejecutar la GUI.

Plataformas admitidas

- Solaris 10 10/09 (actualización 8) x86
- Solaris 10 9/10 (actualización 9) SPARC
- Solaris 10 9/10 (actualización 9) x86
- Microsoft Windows 7 Business
- Microsoft Windows 7 Enterprise
- Microsoft Windows Vista Business
- Microsoft Windows XP Professional versión 2002
- Microsoft Windows XP Professional
- Microsoft Windows Server 2008 versión 6.0
- Microsoft Windows Server 2003 R2 Standard Edition
- Microsoft Windows Server 2003

2.4. CLI de OKM

Dos utilidades de interfaz de línea de comandos (CLI) que admiten un subconjunto de las mismas funciones que la GUI de OKM. Permiten la automatización de diversas tareas,

como creación de copias de seguridad, exportación de claves y elaboración de informes de auditoría.

2.5. Cluster de OKM

Un cluster es un conjunto completo de dispositivos de gestión de claves en un sistema. Todos estos dispositivos de gestión de claves se reconocen entre sí y replican información completa. El cluster permite que las unidades de cinta seleccionen dispositivos de gestión de claves para la recuperación de material de claves.

- Puede haber un mínimo de dos[1] y un máximo de 20 dispositivos de gestión de claves en un cluster.
- Las nuevas claves generadas en cualquier sitio se replican al resto de los dispositivos de gestión de claves del cluster.
- Todos los cambios administrativos se propagan al resto de los dispositivos de gestión de claves del cluster.
- Debe tenerse en cuenta el tamaño del cluster al diseñar el sistema para una máxima disponibilidad.
- Varios dispositivos de gestión de claves pueden agruparse en clusters en una red de área amplia, local o privada dedicada.
- Cualquier dispositivo de gestión de claves del cluster puede proporcionar servicios a cualquier agente de la red.
- Cualquier dispositivo de gestión de claves puede utilizarse para funciones de administración.

Nota:

Los dispositivos de gestión de claves de un cluster desconocen los dispositivos de gestión de claves de otros clusters.

2.5.1. Utilización de dispositivos de gestión de claves por parte de las unidades de cinta en un cluster

Las unidades de cinta recuperan claves del cluster del dispositivo de gestión de claves mediante la detección, el equilibrio de cargas y el failover.

2.5.1.1. Detección

Las unidades de cinta (agentes) envían una solicitud de detección de cluster a un dispositivo de gestión de claves. El dispositivo de gestión de claves que recibe la solicitud de detección de cluster proporciona la siguiente información a cada dispositivo de gestión de claves:

- Dirección IP (IPv4 e IPv6)
- Nombre del sitio
- ID del dispositivo de gestión de claves

[1]Pueden realizarse excepciones con la aprobación de los servicios de soporte, los servicios profesionales y el Departamento de Ingeniería.

- Nombre del dispositivo de gestión de claves
- Versión del dispositivo de gestión de claves (ayuda a determinar la compatibilidad de FIPS para las unidades de cinta admitidas)
- Estado del dispositivo de gestión de claves:
  - Responde: indica si el dispositivo de gestión de claves está respondiendo en la red
  - Bloqueado: indica si el dispositivo de gestión de claves está bloqueado

Las unidades de cinta recuperan periódicamente esta información como parte de una operación de cinta (no cuando la unidad de cinta está inactiva) y siempre la solicitan como parte de la inscripción y cada vez que se realiza la IPL de la unidad.

Cuando la unidad detecta un nuevo estado de respuesta para un dispositivo de gestión de claves, actualiza la información del cluster con el nuevo estado.

2.5.1.2. Equilibrio de carga

Durante operaciones normales de la unidad de cinta, la unidad usa la tabla local de información del cluster para seleccionar un dispositivo de gestión de claves para la recuperación de claves.

Las unidades usan un algoritmo para seleccionar un dispositivo de gestión de claves del mismo sitio que la unidad. Si todos los dispositivos de gestión de claves dentro de un sitio están bloqueados o no responden, la unidad de cinta intenta acceder a un dispositivo de gestión de claves de otro sitio. Si no se puede acceder a los dispositivos de gestión de claves de otros sitios, se producirá el timeout del intento de recuperación de claves y se realizará un failover forzado.

2.5.1.3. Failover

La capacidad de las unidades de cinta de realizar un failover a sitios remotos puede mejorar la confiabilidad y la disponibilidad de la unidad cuando los dispositivos de gestión de claves locales no funcionan o tardan en responder (como en situaciones de timeout causadas por cargas de trabajo intensas).

Cuando una unidad de cinta no puede comunicarse con ninguno de los dispositivos de gestión de claves de un cluster, la unidad usa un algoritmo para seleccionar un dispositivo de gestión de claves para un intento de failover. Al realizar la selección, la información de la unidad sobre el estado del cluster se utiliza nuevamente.

Las unidades de cinta intentan realizar un failover hasta tres veces antes de darse por vencidas y devolver un error a la aplicación host de la unidad de cinta.

Nota:

A veces, es posible que una unidad elija un dispositivo de gestión de claves que no responde durante un intento de failover si el resto de los dispositivos de gestión de claves no responden. Sin embargo, dado que es posible que la información acerca del cluster sea obsoleta, el dispositivo de gestión de claves puede estar en línea y responder.

2.6. Agentes

Los agentes son puntos finales de cifrado que usan claves criptográficas para cifrar y descifrar datos. Los agentes son dispositivos (por ejemplo, unidades de cinta) que se autentican con OKM y obtienen material de claves mediante una sesión "segura" (TLS). Los agentes se comunican con los dispositivos de gestión de claves a través de la API de agente. (La API de agente es un conjunto de interfaces de software incorporadas en el software o hardware del agente). De forma predeterminada, los dispositivos de gestión de claves locales (si están disponibles) proporcionan servicios a los agentes.

- Los agentes de unidad de cinta no deben estar en redes públicas.
- Los agentes deben permanecer conectados a la red en caso de que se necesite una clave de cifrado. Conecte agentes de unidad de cinta a los dispositivos de gestión de claves en una red de servicio privada.
- Los dispositivos de gestión de claves y los agentes pueden "agruparse" lógicamente para crear un sitio, donde los agentes hacen referencia a los dispositivos de gestión de claves dentro del sitio al cual están asignados.

2.7. Unidades de datos, claves, políticas de claves y grupos de claves

Unidades de datos
Las unidades de datos representan los datos cifrados por los agentes. Para las unidades de cinta, una unidad de datos es un cartucho de cinta.

Claves
Las claves son los valores reales de las claves (material de claves) y los metadatos asociados.

Políticas de claves
Las políticas de claves definen los parámetros que rigen las claves. Esto incluye parámetros de ciclo de vida (como período de cifrado y período criptográfico) y parámetros de importación/exportación (por ejemplo, importación permitida, exportación permitida).

Grupos de claves
Los grupos de claves asocian claves y políticas de claves. Cada grupo de claves tiene una política de claves y está asignado a los agentes. Los agentes pueden recuperar solamente las claves que están asignadas a uno de los grupos de claves permitidos del agente. Los agentes también tienen un grupo de claves predeterminado. Cuando un agente crea una clave (la asigna a una unidad de datos), la clave se coloca en el grupo de claves predeterminado del agente.

Nota:

Para que el sistema funcione, debe definir al menos una política de claves y un grupo de claves (asignado como grupo de claves predeterminado) para todos los agentes.

2.8. Roles de usuario

OKM tiene un conjunto predefinido de roles de usuario:

Responsable de la seguridad
Lleva a cabo la gestión y configuración de OKM.

Operador
Lleva a cabo la configuración de los agentes y las operaciones diarias.

Responsable del cumplimiento
Define grupos de claves y controla el acceso de los agentes a los grupos de claves.

Operador de copias de seguridad
Lleva a cabo operaciones de copia de seguridad.

Auditor
Supervisa las pistas de auditoría del sistema.

Miembro del quórum
Visualiza y aprueba las operaciones de quórum pendientes.

Para obtener más información acerca de los roles de usuario, incluida una lista de las operaciones llevadas a cabo por cada rol, consulte la *Guía de administración*.

Nota:

Puede usar una hoja de trabajo para facilitar la planificación de roles de usuario, como la que se incluye en el *Manual de servicio e instalación* de OKM (solo para uso interno). Consulte con el representante de soporte de Oracle.

2.9. Integración de IBM ICSF

IBM Integrated Cryptography Service Facility (ICSF) es una solución de cifrado con un almacén de claves externo que reside en un mainframe de IBM y al cual se puede acceder mediante un protocolo TLS/XML. Para obtener más información, consulte la *Guía de integración de OKM-ICSF*.

3 Configuraciones de OKM

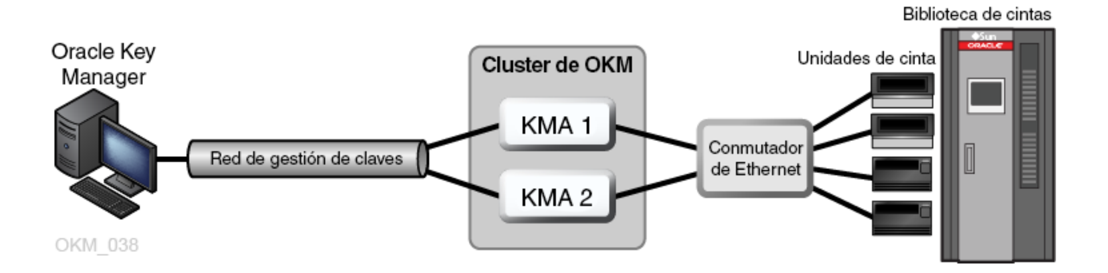
A continuación, se muestran ejemplos de configuraciones de OKM:

- Sitio único
- Dos sitios
- Dos sitios con recuperación ante desastres
- Dos sitios con base de datos Oracle
- Varios sitios con una biblioteca particionada

3.1. Sitio único

En la Figura 3.1, “Configuración de sitio único”, se muestra un sitio único con dos dispositivos de gestión de claves en un cluster. La red de servicio incluye varias unidades de cinta (agentes).

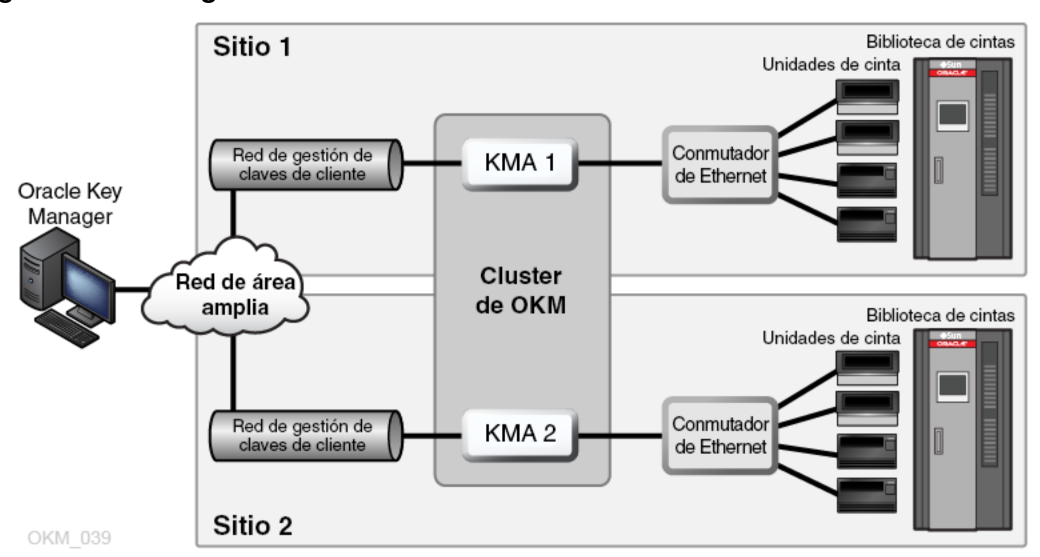
Figura 3.1. Configuración de sitio único



3.2. Dos sitios

En la Figura 3.2, “Configuración de dos sitios”, cada sitio contiene un dispositivo de gestión de claves. Los dispositivos de gestión de claves son gestionados a través de una red de área amplia y ambos dispositivos de gestión de claves pertenecen al mismo cluster de OKM. En esta configuración, Oracle recomienda utilizar sitios separados geográficamente.

Figura 3.2. Configuración de dos sitios



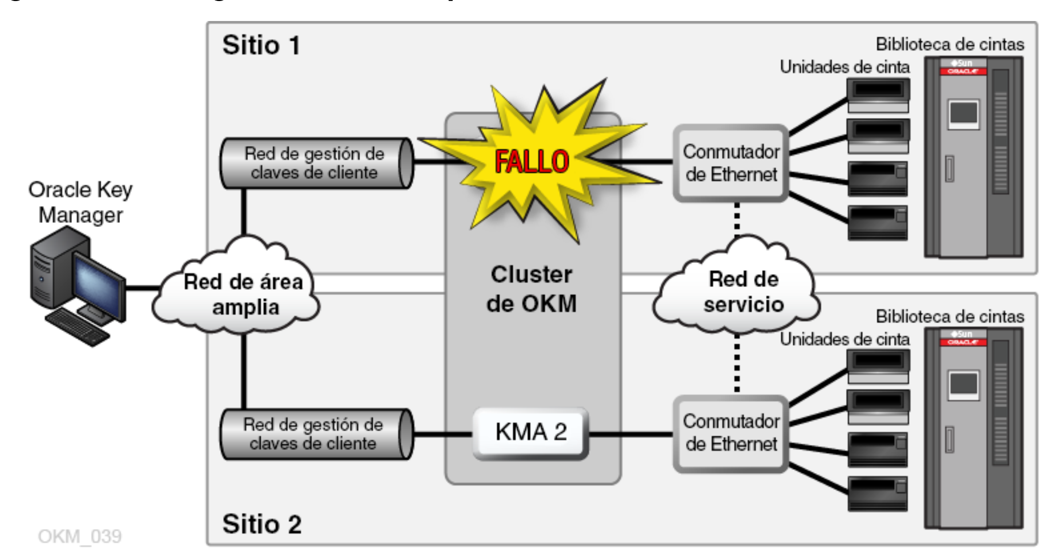
3.3. Dos sitios con recuperación ante desastres

Para reducir el riesgo de que un desastre destruya todo el cluster, el cluster debe abarcar varios sitios separados geográficamente.

En la Figura 3.3, "Configuración de recuperación ante desastres", hay dos redes de área amplia, una para la gestión de claves y una para el servicio. La GUI de OKM se comunica con ambos dispositivos de gestión de claves del cluster y la red de servicio de área amplia permite que cualquiera de los dispositivos de gestión de claves se comunique con los agentes.

Para obtener más información acerca de la recuperación ante desastres, consulte la *Guía de referencia para la recuperación ante desastres*.

Figura 3.3. Configuración de recuperación ante desastres



3.4. Dos sitios con base de datos Oracle

En la Figura 3.4, “Ejemplo de base de datos”, cuatro dispositivos de gestión de claves en un cluster admiten dos bibliotecas de cinta automatizadas y una base de datos Oracle con la solución de cifrado de datos transparente (TDE) de Advanced Security. Para obtener más información, consulte la *Guía de administración* de OKM.

Figura 3.4. Ejemplo de base de datos

3.5. Varios sitios con una biblioteca particionada

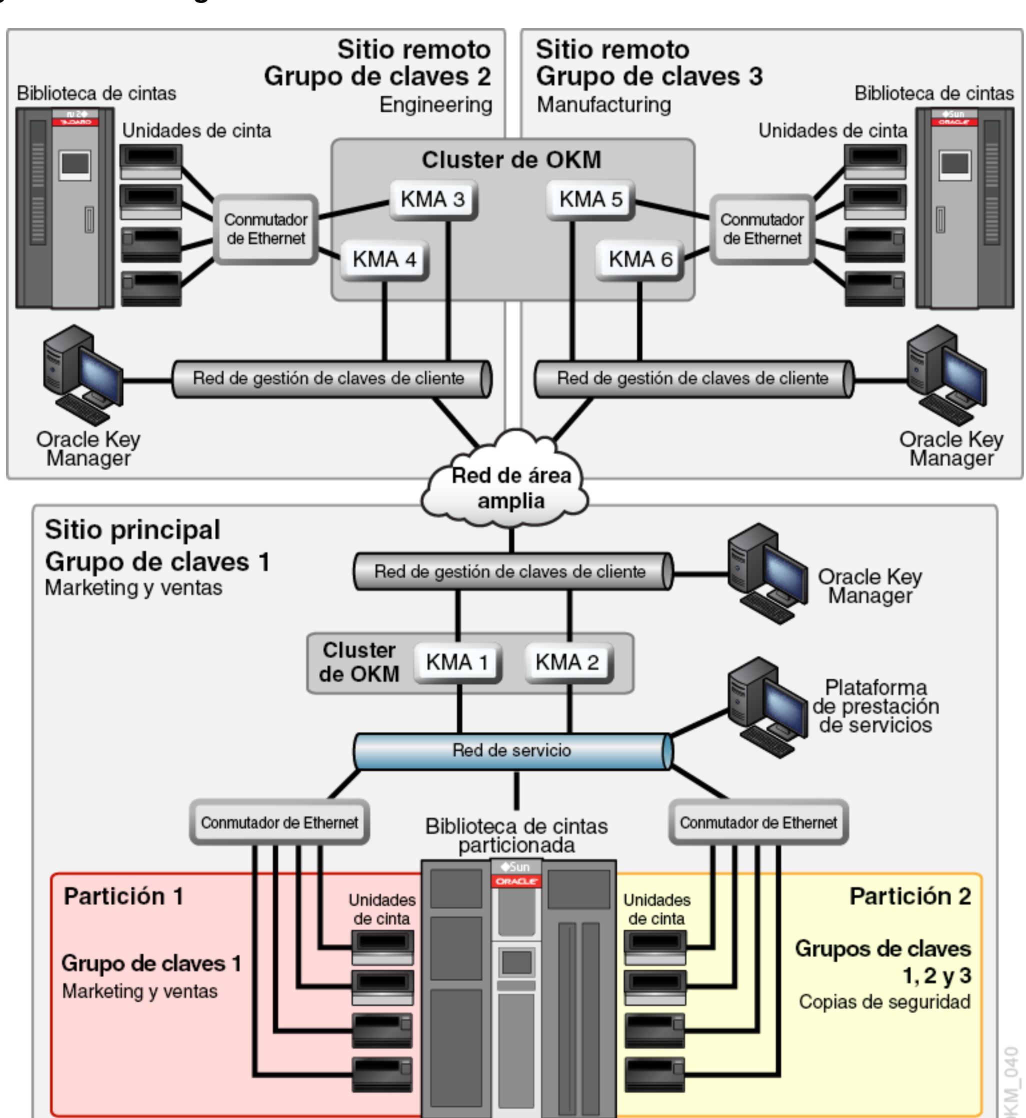
Al usar unidades de cinta con capacidad de cifrado, las particiones pueden agregar una capa de seguridad de datos. Las particiones pueden:

- Limitar el acceso a las unidades de cinta y los cartuchos de cinta.
- Separar distintos grupos de claves de cifrado.
- Aislar clientes como centros de servicio.
- Estar destinadas a tareas específicas.
- Otorgar a varios departamentos, organizaciones y empresas acceso a recursos de la biblioteca con un tamaño adecuado.

En la Figura 3.5, “Configuración de varios sitios”, se muestran dos sitios remotos y un sitio local (principal) dentro de un cluster de OKM. El sitio principal contiene una biblioteca particionada con grupos de claves específicos que proporcionan funciones de copia de seguridad para todos los dispositivos de gestión de claves (1–6) y los medios dentro del cluster.

Para obtener más información acerca de las particiones, consulte la documentación de la biblioteca.

Figura 3.5. Configuración de varios sitios



4

Redes de OKM

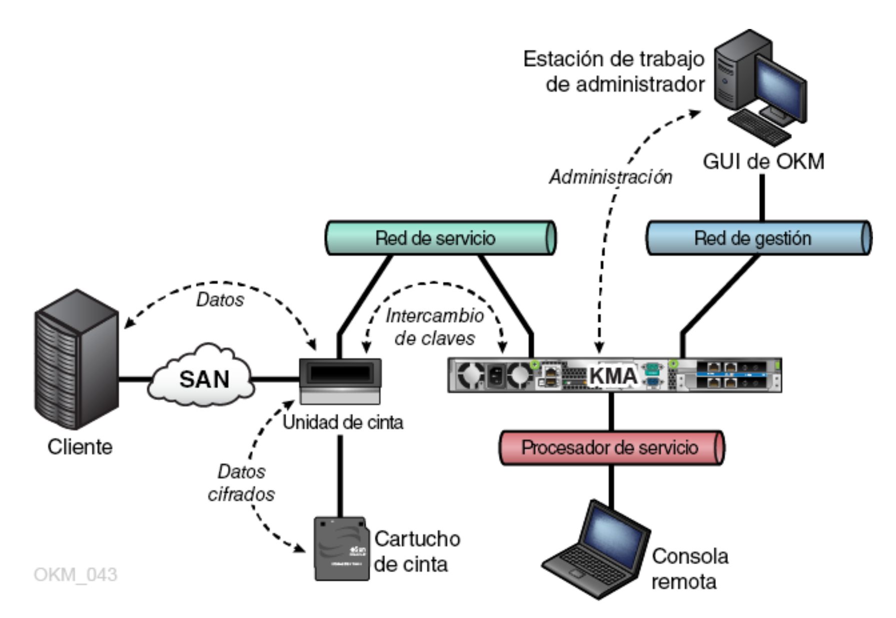
- Descripción general de redes
- Conmutadores gestionados
- Configuración del enrutamiento de red
- Requisitos de firewall de SDP

4.1. Descripción general de redes

OKM usa redes TCP/IP (IPv4 e IPv6 de doble pila[1]) para las conexiones entre dispositivos de gestión de claves, agentes y estaciones de trabajo. Cada dispositivo de gestión de claves tiene conexiones de red para lo siguiente:

- Red de gestión
- Red de servicio
- Procesador de servicio

Figura 4.1. Conexiones de red de OKM



[1]No todas las aplicaciones usan IPv6 (por ejemplo, DNS). Por lo tanto, aún se requiere IPv4.

4.1.1. Red de gestión

Esta red de gestión conecta el dispositivo de gestión de claves a la GUI de OKM y a otros dispositivos de gestión de claves del cluster para una replicación entre pares. La red de gestión puede ser local, remota o una combinación de ambas. Se espera que los clientes proporcionen la red de gestión. Use una conexión Gigabit Ethernet para una replicación y un rendimiento óptimos.

Para una mayor seguridad y para aislar el tráfico LAN, puede utilizar redes de área local virtuales (VLAN) para conectarse a la red de gestión.

4.1.2. Red de servicio

La red de servicio conecta los dispositivos de gestión de claves a los agentes. Aísla las recuperaciones de claves de otro tráfico de red.

De manera opcional, se pueden agregar interfaces de red de servicio del dispositivo de gestión de claves (consulte Sección 4.2.2, “Agregación de puertos de servicio del dispositivo de gestión de claves ”).

4.1.3. Procesador de servicio

La conexión del procesador de servicio permite acceder a Integrated Lights Out Manager (ILOM) en servidores Netra SPARC T4-1 o a Embedded Lights Out Manager (ELOM) en servidores Sun Fire. El representante de soporte de Oracle accede a ILOM/ELOM para la configuración inicial del dispositivo de gestión de claves.

La red del procesador de servicio (ELOM o ILOM) debe tener el árbol de expansión apagado o desactivado.

4.2. Conmutadores gestionados

Oracle recomienda utilizar un conmutador gestionado para conectar los dispositivos de gestión de claves a las unidades de cinta en redes de servicio privadas. Un conmutador gestionado proporciona conectividad a los conmutadores de unidad de cinta no gestionados y a los enrutadores para la red de servicio de área amplia.

Los conmutadores gestionados mejoran el mantenimiento gracias a un mejor diagnóstico y resolución de problemas de la red de servicio, y pueden minimizar puntos únicos de error en la red de servicio mediante el uso de conexiones redundantes y el protocolo de árbol de expansión.

4.2.1. Modelos de conmutadores gestionados admitidos

Oracle prueba, recomienda y proporciona orientación para la configuración de lo siguiente:

- Conmutador 3COM 4500G de 24 puertos (3CR17761-91)
- Extreme Networks Summit X150-24t
- Brocade ICX 6430

4.2.2. Agregación de puertos de servicio del dispositivo de gestión de claves

Puede agregar interfaces Ethernet físicas en una única interfaz virtual. Al agregar estos puertos, se ofrece disponibilidad adicional: si se produce un fallo en alguno de los puertos, el otro puerto mantiene la conectividad.

Asegúrese de que los puertos del conmutador Ethernet estén configurados correctamente. Los puertos del conmutador deben estar configurados para negociar automáticamente el modo de dúplex completo y la velocidad en gigabits.

Para obtener instrucciones de configuración y agregación de puertos de servicio, el representante de soporte de Oracle puede consultar el *Manual de instalación y servicio de OKM* (solo para uso interno).

4.2.3. Creación de reflejos de puertos

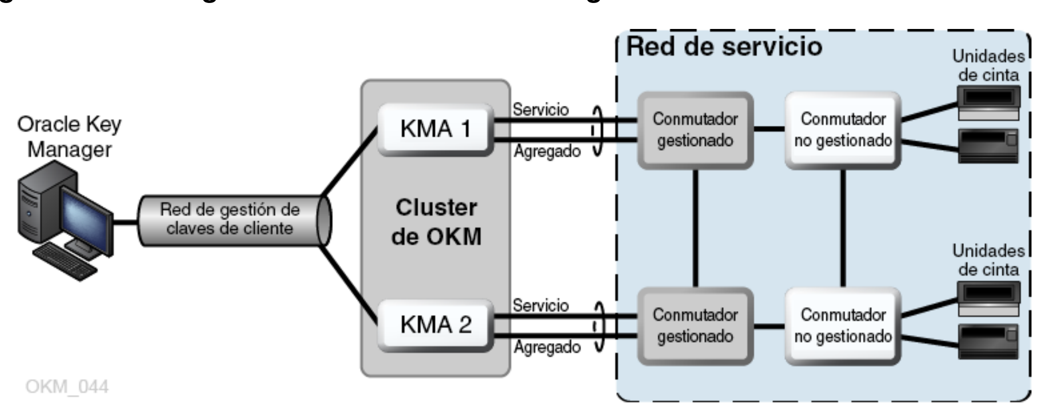
Puede crear reflejos de puertos para usar un analizador de red en la red de servicio. Los puertos se pueden reflejar en conmutadores Brocade ICX 6430. Para obtener instrucciones de configuración, el representante de soporte de Oracle puede consultar el *Manual de instalación y servicio de OKM* (solo para uso interno).

4.2.4. Ejemplo de configuración de conmutadores gestionados

En la Figura 4.2, “Configuración de conmutadores gestionados”:

- Si alguno de los dispositivos de gestión de claves o de los conmutadores gestionados falla, las unidades aún tendrán una ruta de comunicación al otro dispositivo de gestión de claves.
- Los conmutadores gestionados están conectados a conmutadores no gestionados que contienen rutas redundantes que requieren una configuración de árbol de expansión. (Los conmutadores gestionados deben admitir el árbol de expansión siempre que el cableado incluya redundancia).
- Las interfaces de red de servicio se agregan en una única interfaz virtual (consulte Sección 4.2.2, “Agregación de puertos de servicio del dispositivo de gestión de claves ”).

Figura 4.2. Configuración de conmutadores gestionados



4.3. Configuración del enrutamiento de red

La configuración de enrutamiento de un dispositivo de gestión de claves afecta las respuestas de las solitudes de detección de unidades de cinta. Si existen errores en la configuración de enrutamiento, puede proporcionarse información de cluster errónea a las unidades de cinta. Como consecuencia, las unidades intentan comunicarse con dispositivos de gestión de claves a los cuales no pueden acceder mediante la red.

Al planificar la red de OKM, tenga en cuenta lo siguiente:

- Use la opción de menú de red de la consola del dispositivo de gestión de claves para configurar una ruta entre los sitios. No configure una ruta predeterminada.

  Nota:

  Oracle no recomienda comenzar con una topología de red de servicio de varios sitios.

- Al planificar una red de servicio de varios sitios, determine un esquema de direcciones de la subred para las unidades y los puertos de servicio del dispositivo de gestión de claves. Debe evitar direcciones de red duplicadas y el uso de redes 172.18.18.x (una convención común).
- El uso de una configuración de puerta de enlace predeterminada puede afectar el rendimiento del failover. Consulte a un ingeniero de redes para planificar la capacidad de failover.

4.4. Requisitos de firewall de SDP

Service Delivery Platform (SDP) consta de un dispositivo inteligente y una red dedicada. Supervisa las bibliotecas de cinta de Oracle y las unidades serie T. SDP realiza un diagnóstico remoto al recopilar eventos de dispositivos y alertar al soporte de Oracle si existe un problema.

Debe existir un firewall entre los dispositivos conectados a un dispositivo de gestión de claves y SDP. El firewall realiza dos particiones de la red de servicio: la red de servicio

controlada por Oracle y la red de servicio controlada por el cliente. El firewall del cliente permite que SDP acceda únicamente a los dispositivos que puede supervisar.

Importante:

Configure el firewall de modo que SDP pueda supervisar las unidades de cinta en la parte de la red de servicio controlada por el cliente.

En la Figura 4.3, "Ejemplo de conectividad de SDP ":

- El firewall del cliente está conectado al puerto 2 del dispositivo de SDP.

  La interfaz de red del cliente es la conexión entre SDP y los dispositivos de almacenamiento de Oracle conectados a la LAN del centro de operaciones que está conectada a la red. Estos dispositivos incluyen las unidades de cinta y los conmutadores conectados a los dispositivos de gestión de claves.
- La interfaz de red de servicio de Oracle está conectada al puerto 1 del dispositivo de SDP.

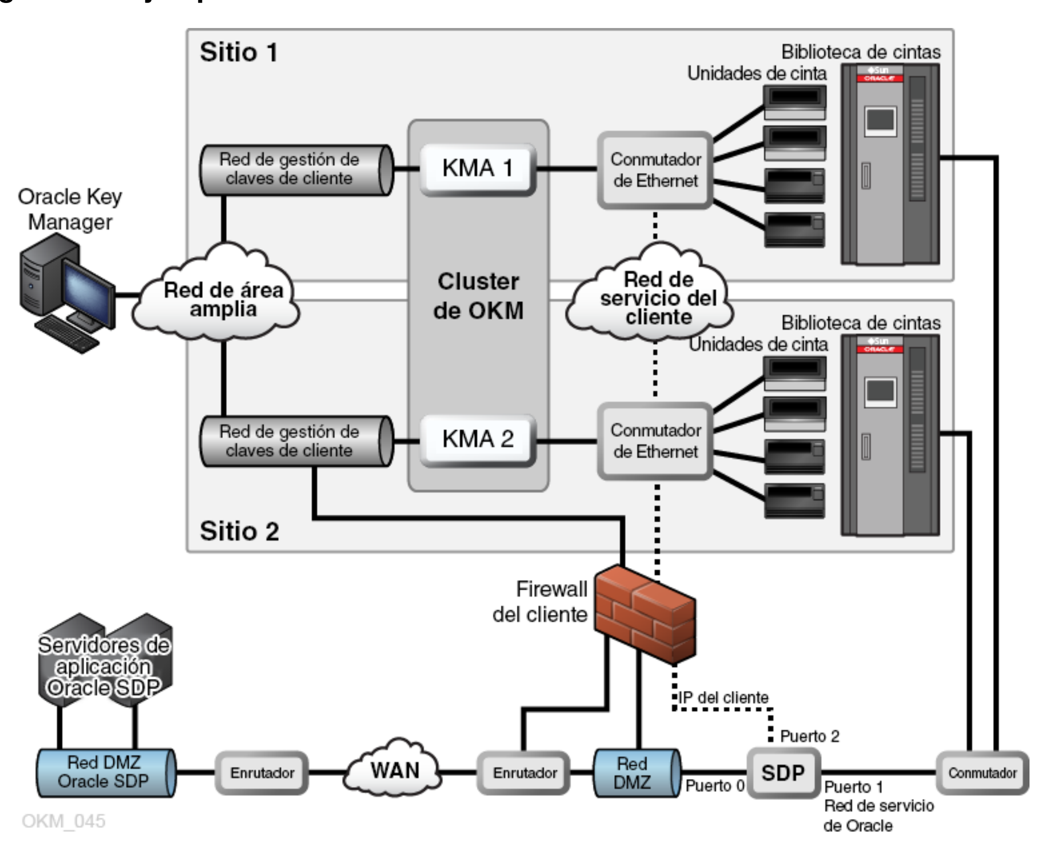
  La interfaz de red de servicio de Oracle es la conexión entre la unidad del sitio SDP y los dispositivos de almacenamiento.
- DMZ se refiere a la arquitectura de red segura de SDP que protege el tráfico de red entre la unidad del sitio SDP y la red de Oracle (puerto 0).

Nota:

El personal del servicio de asistencia de Oracle deberá ocuparse de los equipos en ambas particiones de la red de servicio y coordinar con los ingenieros de SDP la planificación y la configuración.

Para obtener más información, consulte las *Notas del producto de Service Delivery Platform*.

Figura 4.3. Ejemplo de conectividad de SDP



5

Requisitos de unidad de cinta

5.1. Unidades de cinta compatibles

Las siguientes unidades de cinta admiten el cifrado:

- StorageTek T10000A
- StorageTek T10000B
- StorageTek T10000C
- StorageTek T10000D
- StorageTek T9840D
- HP LTO-4 (requiere tarjeta HP Dione)
- HP LTO-5 y 6
- IBM LTO-4, 5 y 6 (todas requieren tarjeta IBM Belisarius)

5.2. Unidades de cinta que cumplen con FIPS

Tabla 5.1. Unidades de cinta que cumplen con FIPS 140-2

Unidad de cinta	Nivel de FIPS 140-2
T10000A	1
T10000B	2
T10000C	1
T10000D	1
T9840D	1
LTO4 (HP e IBM)	Sin planes para FIPS
LTO5 (HP e IBM)	Sin planes para FIPS

Unidad de cinta	Nivel de FIPS 140-2
LTO6 (HP e IBM)	Sin planes para FIPS

Nota:

Las unidades LTO pueden ser validadas por FIPS, pero no necesariamente en aplicaciones de cifrado específicas.

Los niveles de seguridad de FIPS 140-2 para las unidades de cinta antes mencionadas incluyen:

- Nivel 1: el nivel básico con los requerimientos del nivel de producción.
- Nivel 2: agrega requerimientos para pruebas de alteración física y autenticación basada en roles. Basado en una plataforma operativa validada. Esta selección proporciona un mayor nivel de seguridad para los dispositivos de gestión de claves y las unidades de cinta.

5.3. Comportamiento de cifrado de la unidad de cinta serie T

Tabla 5.2. Comportamiento de cifrado de la unidad de cinta serie T

Tipo de unidad de cinta	Cintas no cifradas	Cintas cifradas
No inscrita para cifrado	• Totalmente compatible • Lectura, escritura y conexión	• Sin capacidad de lectura, escritura ni conexión • Se puede volver a escribir desde el inicio de la cinta (BOT)
Inscrita para cifrado	• Capacidad de lectura únicamente • Sin capacidad de conexión • Se puede volver a escribir desde el inicio de la cinta (BOT)	• Totalmente compatible • Lectura con las claves correctas • Escritura con la clave de escritura actual

5.4. Comportamiento de cifrado de unidades LTO

Nota:

Únicamente los medios LTO-4 (LTO-4 y LTO-4 WORM) tienen capacidad de cifrado en las unidades de cinta LTO-4.

Tabla 5.3. Comportamiento de cifrado para unidad LTO-4 no inscrita para cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos no cifrados de LTO-4	Correcto, no cifrado
Leer datos cifrados de LTO-4	Error
Escribir en LTO-4 desde BOT	Correcto, no cifrado
Leer cinta LTO-3	Correcto, no cifrado
LTO-4, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-4, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	Correcto, no cifrado
LTO-4, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, no cifrado

Comportamiento de la unidad	Funcionalidad
LTO-4, agregar escritura a datos cifrados (leer hasta EOD y escribir)	Error

Tabla 5.4. Comportamiento de cifrado para unidad LTO-4 inscrita para cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos no cifrados de LTO-4	Correcto, no cifrado
Leer datos cifrados de LTO-4	Correcto, cifrado si está disponible la clave correcta
Escribir en LTO-4 desde BOT	Correcto, cifrado si está disponible la clave correcta
LTO-4, agregar escritura a datos cifrados	Correcto, cifrado si está disponible la clave correcta
Escribir en cinta LTO-3	HP: correcto, no cifrado[1] IBM: error
Leer cinta LTO-3	Correcto, no cifrado
LTO-4, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[2] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-4, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[2] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-4, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, cifrado si está disponible la clave correcta
LTO-4, agregar escritura a datos cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta IBM: correcto, cifrado si está disponible la clave correcta, pero con clave de lectura anterior[3]

[1]Las unidades HP escribirán cintas en modo no cifrado. El formato LTO-3 no admite el cifrado y esto puede considerarse un incumplimiento de la seguridad, ya que es posible hacer que las unidades HP LTO-4 y 5 escriban datos no cifrados simplemente insertando un cartucho LTO-3.

[2]Aunque este escenario permite agregar datos cifrados detrás de datos no cifrados, esto tiene un beneficio operativo, ya que permite que las cintas etiquetadas previamente con datos no cifrados se utilicen en unidades HP LTO en el entorno de cifrado sin que sea necesario volver a etiquetarlas.

[3]En este escenario, las unidades IBM escribirán datos cifrados, pero utilizarán la misma clave que utilizaron para leer los datos cifrados anteriores en la cinta. La unidad no solicitará una nueva clave de OKM cuando se ejecuta el comando de escritura y se ignorará la política de caducidad de claves definida por OKM.

Tabla 5.5. Comportamiento de cifrado para unidad LTO-5 no inscrita para cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos no cifrados de LTO-5	Correcto, no cifrado
Leer datos cifrados de LTO-5	Error
Escribir en LTO-5 desde BOT	Correcto, no cifrado
Leer datos no cifrados de LTO-4	Correcto, no cifrado
Leer datos cifrados de LTO-4	Error
Escribir en LTO-4 desde BOT	Correcto, no cifrado

Comportamiento de la unidad	Funcionalidad
Leer LTO-3	Correcto, no cifrado
LTO-5, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-5, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	Correcto, no cifrado
LTO-5, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-5, agregar escritura a datos cifrados (leer hasta EOD y escribir)	Error
LTO-4, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-4, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	Correcto, no cifrado
LTO-4, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-4, agregar escritura a datos cifrados (leer hasta EOD y escribir)	Error

Tabla 5.6. Comportamiento de cifrado para unidad LTO-5 inscrita para cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos no cifrados de LTO-5	Correcto, no cifrado
Leer datos cifrados de LTO-5	Correcto, cifrado si está disponible la clave correcta
Escribir en LTO-5 desde BOT	Correcto, cifrado si está disponible la clave correcta
LTO-5, agregar escritura a datos cifrados	Correcto, cifrado si está disponible la clave correcta
Leer datos no cifrados de LTO-4	Correcto, no cifrado
Leer datos cifrados de LTO-4	Correcto, cifrado si está disponible la clave correcta
Escribir en LTO-4 desde BOT	Correcto, cifrado si está disponible la clave correcta
LTO-4, agregar escritura a datos cifrados	Correcto, cifrado si está disponible la clave correcta
LTO-5, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-5, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-5, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, cifrado si está disponible la clave correcta
LTO-5, agregar escritura a datos cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta IBM: correcto, cifrado si está disponible la clave correcta, pero con clave de lectura anterior[2]
LTO-4, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-4, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.

Comportamiento de la unidad	Funcionalidad
LTO-4, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, cifrado si está disponible la clave correcta
LTO-4, agregar escritura a datos cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta IBM: correcto, cifrado si está disponible la clave correcta, pero con clave de lectura anterior[2]
Leer datos no cifrados de LTO-3	Correcto, no cifrado

[1]Aunque este escenario permite agregar datos cifrados detrás de datos no cifrados, esto tiene un beneficio operativo, ya que permite que las cintas etiquetadas previamente con datos no cifrados se utilicen en unidades HP LTO en el entorno de cifrado sin que sea necesario volver a etiquetarlas.

[2]En este escenario, las unidades IBM escribirán datos cifrados, pero utilizarán la misma clave que utilizaron para leer los datos cifrados anteriores en la cinta. La unidad no solicitará una nueva clave de OKM cuando se ejecuta el comando de escritura y se ignorará la política de caducidad de claves definida por OKM.

Tabla 5.7. Comportamiento de cifrado para unidad LTO-6 no inscrita para cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos no cifrados de LTO-6	Correcto, no cifrado
Leer datos cifrados de LTO-6	Error
Escribir en LTO-6 desde BOT	Correcto, no cifrado
Leer datos no cifrados de LTO-5	Correcto, no cifrado
Leer datos cifrados de LTO-5	Error
Escribir en LTO-5 desde BOT	Correcto, no cifrado
Leer datos no cifrados de LTO-4	Correcto, no cifrado
LTO-6, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-6, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	Correcto, no cifrado
LTO-6, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-6, agregar escritura a datos cifrados (leer hasta EOD y escribir)	Error
LTO-5, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-5, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	Correcto, no cifrado
LTO-5, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, no cifrado
LTO-5, agregar escritura a datos cifrados (leer hasta EOD y escribir)	Error

Tabla 5.8. Comportamiento de cifrado para unidad LTO-6 inscrita para cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos no cifrados de LTO-6	Correcto, no cifrado
Leer datos cifrados de LTO-6	Error
Escribir en LTO-6 desde BOT	Correcto, no cifrado
Leer datos no cifrados de LTO-6	Correcto, no cifrado
Leer datos cifrados de LTO-6	Correcto, cifrado si está disponible la clave correcta
Escribir en LTO-6 desde BOT	Correcto, cifrado si está disponible la clave correcta
LTO-6, agregar escritura a datos cifrados	Correcto, cifrado si está disponible la clave correcta
Leer datos no cifrados de LTO-5	Correcto, no cifrado

Comportamiento de la unidad	Funcionalidad
Leer datos cifrados de LTO-5	Correcto, cifrado si está disponible la clave correcta
Escribir en LTO-5 desde BOT	Correcto, cifrado si está disponible la clave correcta
LTO-5, agregar escritura a datos cifrados	Correcto, cifrado si está disponible la clave correcta
Leer datos no cifrados de LTO-4	Correcto, no cifrado
Leer datos cifrados de LTO-4	Correcto, cifrado si está disponible la clave correcta
LTO-6, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-6, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-6, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, cifrado si está disponible la clave correcta
LTO-6, agregar escritura a datos cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta IBM: correcto, cifrado si está disponible la clave correcta, pero con clave de lectura anterior[2]
LTO-5, agregar escritura a datos no cifrados (ir hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-5, agregar escritura a datos no cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta[1] IBM: error. No se permite la combinación de datos cifrados y no cifrados en una sola cinta.
LTO-5, agregar escritura a datos cifrados (ir hasta EOD y escribir)	Correcto, cifrado si está disponible la clave correcta
LTO-5, agregar escritura a datos cifrados (leer hasta EOD y escribir)	HP: correcto, cifrado si está disponible la clave correcta IBM: correcto, cifrado si está disponible la clave correcta, pero con clave de lectura anterior[2]

[1]Aunque este escenario permite agregar datos cifrados detrás de datos no cifrados, esto tiene un beneficio operativo, ya que permite que las cintas etiquetadas previamente con datos no cifrados se utilicen en unidades HP LTO en el entorno de cifrado sin que sea necesario volver a etiquetarlas.

[2]En este escenario, las unidades IBM escribirán datos cifrados, pero utilizarán la misma clave que utilizaron para leer los datos cifrados anteriores en la cinta. La unidad no solicitará una nueva clave de OKM cuando se ejecuta el comando de escritura y se ignorará la política de caducidad de claves definida por OKM.

5.5. Preparación de unidades de cinta para cifrado

Puede inscribir unidades de cinta para cifrado con la ayuda del representante de soporte de Oracle y la *Guía de administración* de OKM. Antes de la inscripción, determinadas unidades requieren preparación. Para obtener más información, los representantes de soporte de Oracle pueden consultar el *Manual de instalación y servicio* de OKM (solo para uso interno).

Preparación de datos de unidades de cinta serie T

Las unidades T10000C y T10000D que ejecutan versiones de firmware 1.57.30x (T10000C) o 4.06.106 (T10000D) y posteriores no requieren claves de activación de cifrado. Para versiones de firmware y unidades anteriores, el representante de soporte de Oracle debe solicitar una clave de licencia de cifrado para cada unidad.

Preparación de unidades de cinta LTO

No existen requisitos de activación ni se requieren datos de unidades para unidades de cinta LTO. La única preparación es asegurarse de contar con información para asignar las direcciones IP y los nombres de agentes para las unidades de cinta en OKM Manager.

5.6. Requisitos de firmware

La Tabla 5.9, “Compatibilidades de firmware ” muestra los requisitos mínimos de firmware para cada unidad de cinta.

Se admiten los siguientes productos de gestión de bibliotecas:

- ACSLS: 7.1 y 7.1.1 con PUT0701, o 7.2 y 7.3
- HSC: 6.1 y 6.2
- VSM: 6.1 o 6.2 (incluye VTCS y VTSS)
- Modelos de VTL: 1.0 o 2.0.

Actualización de firmware

Los niveles de firmware mostrados están sujetos a cambios. Para acceder al firmware más reciente:

1. Vaya a My Oracle Support en `http://support.oracle.com` e inicie sesión.
2. Haga clic en el separador **Patches & Updates** (Parches y actualizaciones).
3. Haga clic en **Product or Family (Advanced)** (Producto o familia [avanzada]).
4. En el campo **Start Typing...** (Comience a escribir...), escriba la información del producto (por ejemplo, "Oracle Key Manager") y haga clic en **Search** (Buscar) para ver el último firmware de cada versión.

Tabla 5.9. Compatibilidades de firmware

Unidades de cinta	SL8500	SL3000	Lxxx	9310/9311	SL500	SL150
T10000A FC	L–3.11c D–1.37.113	L–FRS_2.00 D–1.37.113	L–3.17.03 D–1.37.113	L–4.4.08 D–137113	N/D	N/D
T10000A FICON	L–3.11c D–1.37.114	L–FRS_2.00 D–1.37.114	L–3.17.03 D–1.37.114	L–4.4.08 D–137114	N/D	N/D
T10000B FC	L–3.98b	L–FRS_2.00	L–3.17.03	N/D	N/D	N/D

Unidades de cinta	SL8500	SL3000	Lxxx	9310/9311	SL500	SL150
	D–1.38.x09	D–1.38.x07	D–1.38.x07			
T10000B FICON	L–3.98b D–1.38.x09	L–FRS_2.00 D–1.38.x09	L–3.17.03 D–1.38.x09	N/D	N/D	N/D
T10000C FC	L–FRS_7.0.0 D–1.53.316	L–FRS_3.0.0 D–1.53.316	N/D	N/D	N/D	N/D
T10000C FICON	L–FRS_7.0.0 D–1.53.316	L–FRS_3.0.0 D–1.53.316	N/D	N/D	N/D	N/D
T10000D FC	L–FRS_8.0.5 (sin compatibilidad con la unidad 3590) D–4.06.107 FC/ FCoE	L–FRS_3.62 (sin compatibilidad con la unidad 3590) D–4.06.107 FC/ FCoE	N/D	N/D	N/D	N/D
T10000D FICON	L–FRS_8.0.5 (sin compatibilidad con la unidad 3590) D–4.07.xxx	L–FRS_3.62 (sin compatibilidad con la unidad 3590) D–4.07.xxx	N/D	N/D	N/D	N/D
T10000D FCoE	L_FRS_8.3.0 D–4.06.106	L_FRS_4.xx D_4.06.106	N/D	N/D	N/D	N/D
T9840D FC	L–3.98 D–1.42.x07	L–FRS_2.00 D–1.42.x07	L–3.17.03 D–142x07	L–4.4.08 D–142x07	N/D	N/D
T9840D FICON y ESCON	L–3.98 D–142x07	L–FRS_2.00 D–142x07	L–3.17.03 D–142x07	L–4.4.08 D–142x07	N/D	N/D
HP LTO-4	L–3.98B D–H64S FC N/D para SCSI	L–2.05 D–H64S FC N/D para SCSI	N/D	N/D	L–1300 D–H64S FC D–B63S SCSI	N/D
HP LTO-5	D–I5BS FC N/D para SAS	D–I5BS FC N/D para SAS	N/D	N/D	D–I5BS FC D–X5AS SAS	L–1.80 D–Y5BS FC
HP LTO-6	D– J2AS FC N/D para SAS	D– J2AS FC N/D para SAS	N/D	N/D	D– J2AS FC N/D para SAS	L–1.80 D–Z55S SAS D–22CS FC D–329S SAS
IBM LTO-4	L–FRS_4.70 D–BBH4 FC N/D para SCSI	L–FRS_2.30 D–BBH4 FC N/D para SCSI	N/D	N/D	L–1373 D– BBH4 FC D– BBH4 SCSI	N/D
IBM LTO-5	D–BBNH FC	D–BBNH FC	N/D	N/D	L–1373	N/D

Unidades de cinta	SL8500	SL3000	Lxxx	9310/9311	SL500	SL150
					D–BBNH FC	
IBM LTO-6	L–8.01 D–CT94 FC	L–4.0 D–CT94 FC	N/D	N/D	L–1483 D–BBNH FC N/D para FC	N/D

Leyenda:

- L: nivel de firmware de la biblioteca
- D: nivel de firmware de la unidad
- FC: canal de fibra
- FCoE: canal de fibra sobre Ethernet
- SPS: firmware especial, requiere aprobación
- N/D: no disponible. No admitida.

5.7. Requisitos del panel de operador virtual

En la Tabla 5.10, “Versión mínima del VOP”, se muestra la versión mínima del panel de operador virtual (VOP) de Oracle para cada tipo de unidad.

Nota:

Si utiliza un panel de operador virtual de varias unidades (MD-VOP), se requiere la versión 1.1 (como mínimo).

Tabla 5.10. Versión mínima del VOP

Unidad de cinta	Versión mínima del VOP
T10000A, B, C, D	1.0.18
T9840D	1.0.12
HP LTO-4	1.0.12
HP LTO-5	1.0.16
HP LTO-6	1.0.18
IBM LTO-4	1.0.14
IBM LTO-5	1.0.16
IBM LTO-6	1.0.18

6

Realización de pedidos

- Servidor del dispositivo de gestión de claves
- Kit de accesorios del conmutador
- Cables Ethernet
- Cables de alimentación

6.1. Servidor del dispositivo de gestión de claves

Tabla 6.1. Números de pedido de servidores del dispositivo de gestión de claves

Número de pedido	Descripción
7105795	Servidor Netra SPARC T4-1 personalizado para OKM
375-3424-06	Tarjeta Sun Cryptographic Accelerator (SCA6000)

6.2. Kit de accesorios del conmutador

Tabla 6.2. Números de pedido del kit de accesorios del conmutador

Número de pedido	Descripción
7104584	Kit de accesorios del conmutador (SAK). Incluye un conmutador gestionado de 24 puertos, cables y herramientas de montaje.

6.3. Cables Ethernet

Tabla 6.3. Números de pedido de cables Ethernet

Número de pedido	Descripción
CABLE10187033-Z-N	Cable Ethernet CAT5e de 8 ft
CABLE10187034-Z-N	Cable Ethernet CAT5e de 35 ft
CABLE10187037-Z-N	Cable Ethernet CAT5e de 55 ft

6.4. Cables de alimentación

Tabla 6.4. Números de referencia de cables de alimentación

Cable de alimentación ATO	Equivalente PTO	Descripción	Amperios	Tensión	Cable
333A-25-10-AR	X312F-N	Cable de alimentación, Argentina, 2,5 m, IRAM2073, 10 A, C13	10	250	180-1999-02

Cable de alimentación ATO	Equivalente PTO	Descripción	Amperios	Tensión	Cable
333A-25-10-AU	X386L-N	Cable de alimentación, Australia, 2,5 m, SA3112, 10 A, C13	10	250	180-1998-02
333A-25-10-BR	X333A-25-10-BR-N	Cable de alimentación, Brasil, 2,5 m, NBR14136, 10 A, C13	10	250	180-2296-01
333A-25-10-CH	X314L-N	Cable de alimentación, Suiza, 2,5 m, SEV1011, 10 A, C13	10	250	180-1994-02
333A-25-10-CN	X328L	Cable de alimentación, China, 2,5 m, GB2099, 10 A, C13	10	250	180-1982-02
333A-25-10-DK	X383L-N	Cable de alimentación, Dinamarca, 2,5 m, DEMKO107, 10 A, C13	10	250	180-1995-02
333A-25-10-EURO	X312L-N	Cable de alimentación, Europa, 2,5 m, CEE7/VII, 10 A, C13	10	250	180-1993-02
333A-25-10-IL	X333A-25-10-IL-N	Cable de alimentación, Israel, 2,5 m, SI-32, 10 A, C13	10	250	180-2130-02
333A-25-10-IN	X333A-25-10-IN-N	Cable de alimentación, India, 2,5 m, IS1293, 10 A, C13	10	250	180-2449-01
333A-25-10-IT	X384L-N	Cable de alimentación, Italia, 2,5 m, CEI23, 10 A, C13	10	250	180-1996-02
333A-25-10-KR	X312G-N	Cable de alimentación, Corea, 2,5 m, KSC8305, 10 A, C13	10	250	180-1662-03
333A-25-10-TW	X332A-N	Cable de alimentación, Taiwán, 2,5 m, CNS10917, 10 A, C13	10	125	180-2121-02
333A-25-10-UK	X317L-N	Cable de alimentación, Reino Unido, 2,5 m, BS1363A, 10 A, C13	10	250	180-1997-02
333A-25-10-ZA	X333A-25-10-ZA-N	Cable de alimentación, Sudáfrica, 2,5 m, SANS164, 10 A, C13	10	250	180-2298-01
333A-25-15-JP	X333A-25-15-JP-N	Cable de alimentación, Japón, 2,5 m, PSE5-15, 15A, C13	15	125	180-2243-01
333A-25-15-NEMA	X311L	Cable de alimentación, N.A./Asia, 2,5 m, 5-15P, 15 A, C13	15	125	180-1097-02
333A-25-15-TW	X333A-25-15-TW-N	Cable de alimentación, Taiwán, 2,5 m, CNS10917, 15 A, C13	15	125	180-2333-01
333F-20-10-NEMA	X320A-N	Cable de alimentación, N.A./Asia, 2,0 m, 6-15P, 10 A, C13	10	250	180-2164-01
333F-25-15-JP	X333F-25-15-JP-N	Cable de alimentación, Japón, 2,5 m, PSE6-15, 15 A, C13	15	250	180-2244-01
333J-40-15-NEMA	X336L	Cable de alimentación, N.A./Asia, 4,0 m, L6-20P, 15 A, C13	15	250	180-2070-01
333R-40-10-309	X332T	Cable de alimentación, internacional, 4,0 m, IEC309-IP44, 10 A, C13	10	250	180-2071-01

Tabla 6.5. Números de referencia de cables de alimentación de racks que no pertenecen a Oracle

Cable de alimentación ATO	Equivalente PTO	Descripción	Amperios	Tensión	Cable
333V-20-15-C14	X333V-20-15-C14-N	Cable de alimentación, Jmpr, directo, 2,0 m, C14, 15 A, C13	15	250	180-2442-01
333V-30-15-C14	X333V-30-15-C14-N	Cable de alimentación, Jmpr, directo, 3,0 m, C14, 15 A, C13	15	250	180-2443-01

Tabla 6.6. Números de referencia de cables de alimentación de Oracle Rack (NGR)

Cable de alimentación ATO	Equivalente PTO	Descripción	Amperios	Tensión	Cable
333W-10-13-C14RA	X9237-1-A-N	Cable de alimentación, Jmpr, 1,0 m, C14RA, 13 A, C13	13	250	180-2082-01
333W-25-13-C14RA	X9238-1-A-N	Cable de alimentación, Jmpr, 2.5 m, C14RA, 13 A, C13	13	250	180-2085-01

Tabla 6.7. Números de referencia de cables de alimentación de Oracle Rack II (Redwood)

Cable de alimentación ATO	Equivalente PTO	Descripción	Amperios	Tensión	Cable
SR-JUMP-1MC13	XSR-JUMP-1MC13-N	Cable de alimentación, Jmpr, SR2, 1,0 m, C14RA, 13 A, C13	13	250	180-2379-01
SR-JUMP-2MC13	XSR-JUMP-2MC13-N	Cable de alimentación, Jmpr, SR2, 2,0 m, C14RA, 13 A, C13	13	250	180-2380-01